

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/003967

International filing date: 08 March 2005 (08.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-067004
Filing date: 10 March 2004 (10.03.2004)

Date of receipt at the International Bureau: 12 May 2005 (12.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

10. 3. 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 3 月 1 0 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 0 6 7 0 0 4

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

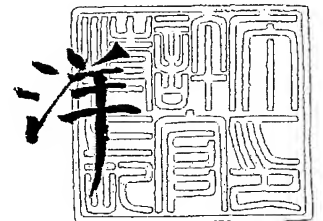
J P 2 0 0 4 - 0 6 7 0 0 4

出 願 人
Applicant(s): 松下電器産業株式会社

2 0 0 5 年 4 月 2 0 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 2048260029
【提出日】 平成16年 3月10日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 12/28
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 ライクセンリング ジェルマーノ
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 金丸 智一
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 大蘆 雅弘
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100097445
 【弁理士】
 【氏名又は名称】 岩橋 文雄
【選任した代理人】
 【識別番号】 100103355
 【弁理士】
 【氏名又は名称】 坂口 智康
【選任した代理人】
 【識別番号】 100109667
 【弁理士】
 【氏名又は名称】 内藤 浩樹
【手数料の表示】
 【予納台帳番号】 011305
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9809938

【書類名】 特許請求の範囲**【請求項 1】**

リソース利用装置からリソース提供装置へのアクセスを制御するアクセス制御装置であって、

リソース利用装置からリソース提供装置へのリソース利用を許可するアクセス制御をリソース提供装置に対して行うアクセス許可部と、

アクセス制御装置とリソース利用装置との通信状態を監視する存在確認部と、

存在確認部にてリソース利用装置とのリンク切断が確認された場合、前記アクセス制御を破棄する破棄制御をリソース提供装置に対して行うアクセス破棄部と、

を備えたアクセス制御装置。

【請求項 2】

上記アクセス許可部にてアクセス制御を行ったリソース利用装置とリソース提供装置との組を管理する許可情報管理手段を備え、

上記存在確認部は、許可情報管理手段にて管理しているリソース利用装置のみとの通信状態を監視することを特徴とする請求項 1 記載のアクセス制御装置。

【請求項 3】

アクセス制御を行ったリソース提供装置のうち、破棄制御を行う必要のあるひとつ以上のリソース提供装置を管理する破棄対象管理手段を備え、

上記存在確認部は、リソース提供装置に対する特定のリソース利用装置のみとの通信状態を監視することを特徴とする請求項 2 記載のアクセス制御装置。

【請求項 4】

アクセス制御装置よりアクセス制御され、リソース利用装置よりリソース利用されるリソース提供装置であって、

リソース利用装置からのリソース利用を許可するアクセス許可部と、

上記リソース提供装置とアクセス制御装置との通信状態を監視する存在確認部と、

存在確認部にてアクセス制御装置とのリンク切断が確認された場合、前記アクセス制御を破棄するアクセス破棄部と、

を備えたリソース提供装置。

【書類名】明細書

【発明の名称】リソース提供装置およびアクセス制御装置

【技術分野】

【0001】

本発明は、電子機器のアクセス制御に関する。

【背景技術】

【0002】

近年、電子機器のマルチユーザ化が進められ、同じ機器でも同時に複数のユーザが使うことが可能になった。ユーザが自身の機器を他人に貸しながら同時に機器を利用することができるようになった。

【0003】

ネットワークを介してユーザが機器を貸し出す場合、セキュリティが最も重要な要素である。物理的な世界であればユーザが自身の手でものを渡し、誰がリソース利用をしているかを管理することができる。しかしネットワークを通した場合、知らない間に自身の機器が不正に他人に使われる恐れがある。

【0004】

非特許文献1はその課題を解決するプロトコルである（以下、「UPnPセキュリティ」とする）。UPnPセキュリティを使うことで、ネットワークを介して電子機器のリソース利用のアクセス制御を行うことができる。リソース利用を制御する機器が、リソースを提供する機器へのアクセス制御命令をネットワーク上通信するための汎用的なプロトコルである。

【0005】

また、UPnPセキュリティでは、アクセス制御を行うときに破棄の条件を設定することができる。具体的に、アクセス制御に対して有効期間を設定することができる。

【0006】

しかしながら、UPnPセキュリティではアクセス制御を与えるときに有効期間がわからない場合は有効ではない。

【0007】

つまりアクセス制御の破棄に関しては速やかに破棄するという技術が十分でない。アクセス制御の破棄は、実世界で破棄すべき状態になってから実際に破棄されるまでの間を限りなく0に近づけなければならない。

【0008】

また、特許文献1では無線通信機能を備えた複数の機器における使用許可を制御する技術が公開されている。特許文献1で定義されている機器グループにおいて、使用許可装置とグループ内のひとつの機器の存在確認ができなくなるとすべての機器を使用不許可にすることができる。

【特許文献1】特開2003-289307号公報

【非特許文献1】UPnP Device Security and Security Console V, UPnP Forum, 2003, <http://www.upnp.org/standardizeddcps/security.asp>

【発明の開示】

【発明が解決しようとする課題】

【0009】

しかしながら、特開2003-289307号公報ではアクセス制御される電子機器をユーザ同士が共有することができないという課題を有していた。

【0010】

本発明は、前記従来の課題を解決するもので、破棄すべきアクセス制御を速やかに破棄し、リソースを提供する機器の不正な使用を防止することを目的とする。

【課題を解決するための手段】

【0011】

前期従来の課題を解決するために、第1の発明によれば、アクセス制御装置は、リソ

ス利用装置からリソース提供装置へのアクセスを許可するアクセス制御を行い、アクセス許可装置とリソース利用装置との通信状態を監視し、リソース利用装置とのリンク切断が確認された場合、前期アクセス制御を破棄する破棄制御をリソース提供装置に対して行うことによって、リソース提供装置の不正な使用を防止することができる。

【0012】

また、アクセス制御装置は、アクセス制御を行ったリソース利用装置とリソース提供装置との組を管理し、管理しているリソース利用装置のみとの通信状態を監視するようにしてもよい。

【0013】

また、アクセス制御装置は、アクセス制御を行ったリソース提供装置のうち、破棄制御を行う必要のあるひとつ以上のリソース提供装置を管理し、リソース提供装置を利用する特定のリソース利用装置のみとの通信状態を監視するようにしてもよい。

【0014】

本発明の第2の発明によれば、リソース提供装置は、アクセス制御装置よりアクセス制御され、リソース利用装置よりリソース利用され、リソース利用装置からのアクセスを許可し、リソース提供装置とアクセス制御装置との通信状態を監視し、存在確認部にてアクセス制御装置とのリンク切断が確認された場合、前期アクセス制御を破棄することによって、リソース提供装置の不正な使用を防止することができる。

【発明の効果】**【0015】**

本発明によれば、破棄すべきアクセス制御を速やかに破棄し、リソースを提供する機器の不正な使用を防止するリソース提供装置20およびアクセス制御装置10を提供することができる。

【発明を実施するための最良の形態】**【0016】**

以下、本発明の実施の形態について、図を用いて説明する。

【0017】

(実施の形態1)

図1は、本発明の実施形態に係るアクセス制御システムの全体構成の一例を示す図である。図1において、アクセス制御システムは3つの電子機器10、20、30と、それぞれの電子機器をつなぐ接続40、50、60とを備える。アクセス制御装置10は、リソース提供装置20との接続40上で通信を行い、リソース提供装置20上に存在するリソースへのアクセスを制御する。リソース利用装置30はリソース提供装置20との接続50上で通信を行い、リソース提供装置20のリソースを利用する。アクセス制御装置10はリソース利用装置30との接続60上で通信を行い、リソース利用装置30の存在確認を行う。存在確認を行うことで、アクセス制御を速やかに破棄できる。

【0018】

接続40、50、60はインターネットなどのネットワークを介した接続や無線通信を使った接続や有線通信を使った接続などを指す。

【0019】

リソース利用とは具体的にリソース提供装置20に対して、記憶データへのアクセスやリソース提供装置20が構成されるデバイスへの入出力などリソース提供装置20の本来の機能を利用しリソース利用装置30に有益な通信を指す。

【0020】

このアクセス制御システムを利用する主な目的はリソース利用装置30からリソース提供装置20への通信を行いリソース利用をすることである。そのリソース利用はアクセス制御装置10の制御のもとで行われる。図2はアクセス制御装置10がアクセス制御を行うシーケンスの一例を示している。

【0021】

リソース利用を制御できるため、アクセス制御装置10とアクセス提供装置は事前準備

を行う必要がある。具体的にリソース提供装置 20 は、アクセスができる機器としてアクセス制御装置 10 を認めている必要がある。その方法は公知のものであり、具体的には非特許文献 1 の方法を採用できる。図 2 では、事前準備がすでに行われていて、リソース提供装置 20 がアクセス制御装置 10 からの命令を認証していて許可があると認めている。

【0022】

アクセス制御装置 10 がアクセス制御を行う場合、アクセス制御装置 10 がリソース提供装置 20 に対してアクセス制御命令を送信する（ステップ S1）。また、アクセス制御装置 10 がリソース利用装置 30 に対してアクセス許可通知命令を送信する（ステップ S2）。ステップ S1 とステップ S2 の順番はこだわらないが、次のステップ S3 を行うためにステップ S1 とステップ S2 が完了している必要がある。

【0023】

尚、ステップ S2 ではアクセス制御装置 10 がリソース利用装置 30 に対してアクセス許可通知を行っているが、実装によってはステップ S2 の代替としてリソース提供装置 20 がリソース利用装置 30 に通知することも考えられる。あるいはユーザによる手動入力も可能である。重要なのはリソース利用装置 30 にリソース利用が許可されたことを通知することである。

【0024】

アクセス制御装置 10 はアクセス制御命令を送信した後リソース利用装置 30 の存在確認を行う（ステップ S3）。ステップ S3 では存在確認が成功しているため、アクセス制御装置 10 はアクセス制御の破棄を行わない。

【0025】

ステップ S1 とステップ S2 が行われた後、リソース利用装置 30 がリソース提供装置 20 に対してアクセス制御が必要なリソースへのアクセス命令を送信できる（ステップ S3）。リソース提供装置 20 はアクセス命令を受信し、アクセス命令のアクセス許可を確認する。許可が認められた場合だけ、アクセス命令に応じてリソース利用が成功する。

【0026】

アクセス制御装置 10 はアクセス制御を送信した後リソース利用装置 30 の存在確認を行い続ける（ステップ S5）。ステップ S5 では存在確認に失敗しているため、アクセス制御装置 10 がアクセス制御の破棄をしなければならないと判断する。

【0027】

存在確認に失敗したため、アクセス制御装置 10 がリソース提供装置 20 に対してアクセス制御破棄命令を送信する（ステップ S6）。リソース提供装置 20 は、アクセス許可破棄命令を処理した後、ステップ S4 で行われていたアクセス命令に対して応じなくなりリソース利用が失敗する。

【0028】

リソース利用が失敗した場合、リソース提供装置 20 がリソース利用装置 30 に対して失敗の理由を示すエラーコードを送信してもよい。

【0029】

図 3 ではアクセス制御命令とアクセス制御通知命令とアクセス制御破棄命令に使われる構造体の一例を示す。構造体は、タイプと機器 ID とひとつ以上の許可情報を持つ。タイプとは、アクセス制御命令かアクセス制御通知命令かアクセス制御破棄命令かを特定する定数である。機器 ID とは具体的に機器の IP アドレスや、機器の公開鍵のハッシュ値や、機器の公開鍵など機器を特定できる ID を指す。制御情報とは、アクセス制御されるコマンド名の名前とコマンドに対するゼロ以上のパラメータ制限からなる。

【0030】

尚、実施によってはアクセス制御命令やアクセス制御通知命令やアクセス制御破棄命令に許可情報を添付しない方法が考えられる。それはたとえば制御される命令やパラメータがシステム設計時に決定される場合が考えられる。

【0031】

尚、上記構造体は一例であり、それぞれの命令が上記構造体に従わなくてもよい。たと

例えば、アクセス制御装置 10 とリソース提供装置 20 の間であらかじめ決められた整理番号を利用し、アクセス制御破棄命令の中身はその整理番号だけで決められるようにしてもよい。そのとき、リソース提供装置 20 は、受信した整理番号に基づいてどのアクセス制御を破棄すべきかを決定する。

【0032】

図 4 ではアクセス制御装置 10 がアクセス制御を行うための動作手順をフローチャートの形式で示している。

【0033】

まずアクセス制御装置 10 はリソース提供装置 20 に対してアクセス制御命令を送信する（ステップ S10）。そしてアクセス制御装置 10 はリソース利用装置 30 に対してアクセス制御通知命令を送信する（ステップ S11）。アクセス許可通知を送信した後、アクセス制御装置 10 がリソース利用装置 30 の存在確認を行い（ステップ S12）、存在が確認できたかどうかの判断を行う（ステップ S13）。存在確認ができた場合、一定時間スリープを行う（ステップ S14）。一定時間スリープした後、存在確認を繰り返す。また、存在確認ができなかったと判断した場合、アクセス制御装置 10 はリソース提供装置 20 に対してアクセス破棄命令を送信しアクセス許可を破棄する（ステップ S15）。

【0034】

アクセス制御装置 10 が複数の機器を同時に監視できるため、許可情報管理テーブルが必要になる。図 5 ではアクセス制御装置 10 が利用する許可情報管理テーブルの一例を示す。

【0035】

提供側の列 100 は、リソースを提供する特定のリソース提供装置 20 との接続の情報が書き込まれる。アクセス制御破棄命令を配信するときに利用する接続である。

【0036】

利用側の列 101 は、リソースを利用する特定のリソース利用装置 30 との接続の情報が書き込まれる。存在確認を行うときに利用する接続である。

【0037】

通信インターフェースの列 102 は、リソース利用装置 30 の存在確認に利用されるひとつ以上のデバイスと通信プロトコルに依存した通信に関する制限を書き込むことができる。たとえば、IP ネットワークで通信を行う場合 2 点の通信において距離を HOP という論理単位で計算することができるので 1 HOP 以内などと制限できる。

【0038】

アクセスの列 103 は、破棄制御対象の制御情報が書き込まれる。

【0039】

上記許可情報管理テーブルに基づいたアクセス制御装置 10 は次の処理を行う。アクセス許可を与えたとき、許可情報管理テーブルに一行を追加する。定期的に許可情報管理テーブルの各行に基づいて存在確認を行い、存在確認ができなかった場合アクセス破棄命令を送信し対象の行を削除する。

【0040】

上記許可情報管理テーブルを使った場合の存在確認およびアクセス制御破棄命令の送信は具体的に次のように行われる。通信インターフェースの列 102 に書いてある通信インターフェースを利用し、利用側の列 101 に書いてある機器の存在確認を順番に行う。存在確認ができなかった列に対してアクセス破棄命令の送信を行う。具体的に提供側の列 100 に書いてあるリソース提供装置 20 に対して利用側の列 101 に書いてあるリソース利用装置 30 によるアクセスの列 103 に書いてあるリソース利用のアクセス制御破棄命令を送信する。そして存在確認ができなかった行を削除する。

【0041】

図 5 の 2 行目の例では、アクセス制御装置 10 は通信インターフェース eth0 を利用し、携帯電話 E の存在確認を行う。そして携帯電話 E の存在確認ができなかった場合、携帯電話 B に対して携帯電話 E による秘密資料参照のアクセス制御破棄命令を送信する。

【0042】

図5の3行目の例では、アクセス制御装置10はすべての通信インターフェースを利用し、携帯電話Bの存在確認を行う。そしてどの通信インターフェースで存在確認を行っても携帯電話Bの存在確認ができなかった場合、据置機器Cに対して携帯電話Bによるビデオ視聴のアクセス制御破棄命令を送信する。

【0043】

ただし、リソース提供装置20とアクセス制御装置10との間の通信が途絶された場合、アクセス制御装置10がリソース提供装置20に対してアクセス制御破棄命令を送信できなくなる。その場合はセキュリティの観点ではリソース提供装置20側でアクセス制御を破棄する必要がある。

【0044】

図6ではリソース提供装置20の動作手順をフローチャートの形式で示している。

【0045】

まずリソース提供装置20はアクセス制御装置10よりアクセス許可命令を受信し、アクセス管理テーブルを変更する(ステップS20)。アクセス許可命令を受信した後、アクセス制御装置10の存在確認をし続ける。具体的にアクセス制御装置10の存在確認を行い(ステップS21)、存在確認ができたかどうかの判断を行う(ステップS22)。存在確認ができた場合、一定時間スリープを行う(ステップS23)。一定時間スリープした後、存在確認を繰り返す。また、存在確認ができなかったと判断した場合、アクセス管理テーブルを変更しアクセス制御を破棄する(ステップS24)。

【0046】

リソース提供装置20が複数の機器を同時に監視できるため、許可情報管理テーブルが必要になる。図7ではリソース提供装置20が利用する許可情報管理テーブルの一例を示す。

【0047】

制御側の列200は、アクセス制御を行う特定のアクセス制御装置10との接続情報が書き込まれる。存在確認を行うときに利用する接続である。

【0048】

アクセスの列201は、破棄制御対象の制御情報が書き込まれる。

【0049】

上記許可情報管理テーブルを使った場合の存在確認およびアクセス制御の破棄は次のように行われる。制御側の列200に書いてある機器の存在確認を順番に行う。存在確認ができなかった行に対してアクセスの列201に書いてあるアクセス制御の破棄を行い、存在確認ができなかった行を削除する。

【0050】

図7の2行目の例では、リソース提供装置20は携帯電話Hの存在確認を行う。そして携帯電話Hの存在確認ができなかった場合、秘密資料参照のアクセス制御を破棄する。

【産業上の利用可能性】**【0051】**

電子機器のアクセス制御に関して、破棄すべきアクセス制御を速やかに破棄し、リソースを提供する機器の不正な使用を防止することに利用可能である。

【図面の簡単な説明】**【0052】**

【図1】本発明の実施形態に係るアクセス制御システムの全体構成の一例を示した図

【図2】アクセス制御装置10がアクセス制御を行うシーケンスの一例を示した図

【図3】アクセス制御命令とアクセス制御通知命令とアクセス制御破棄命令に使われる構造体の一例を示した図

【図4】アクセス制御装置10がアクセス制御を行うための動作手順のフローチャート

【図5】アクセス制御装置10が利用する許可情報管理テーブルの一例を示した図

【図 6】 リソース提供装置の動作手順を示す図

【図 7】 リソース提供装置が利用する許可情報管理テーブルを示す図

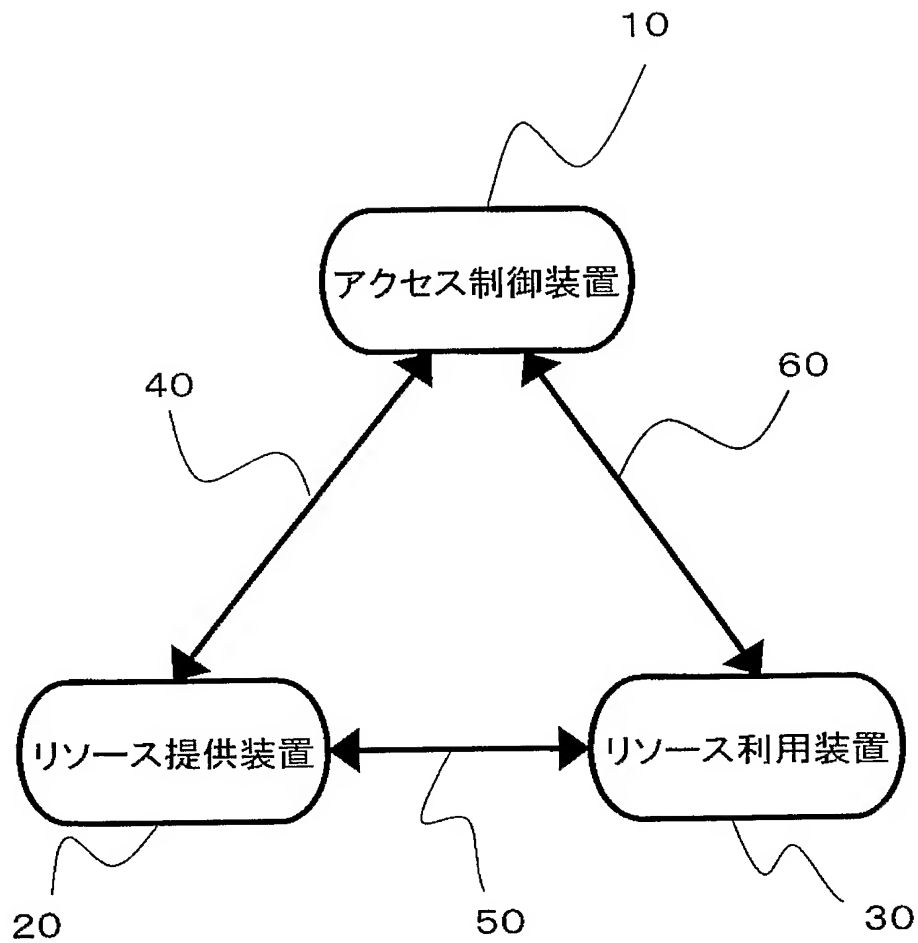
【符号の説明】

【 0 0 5 3 】

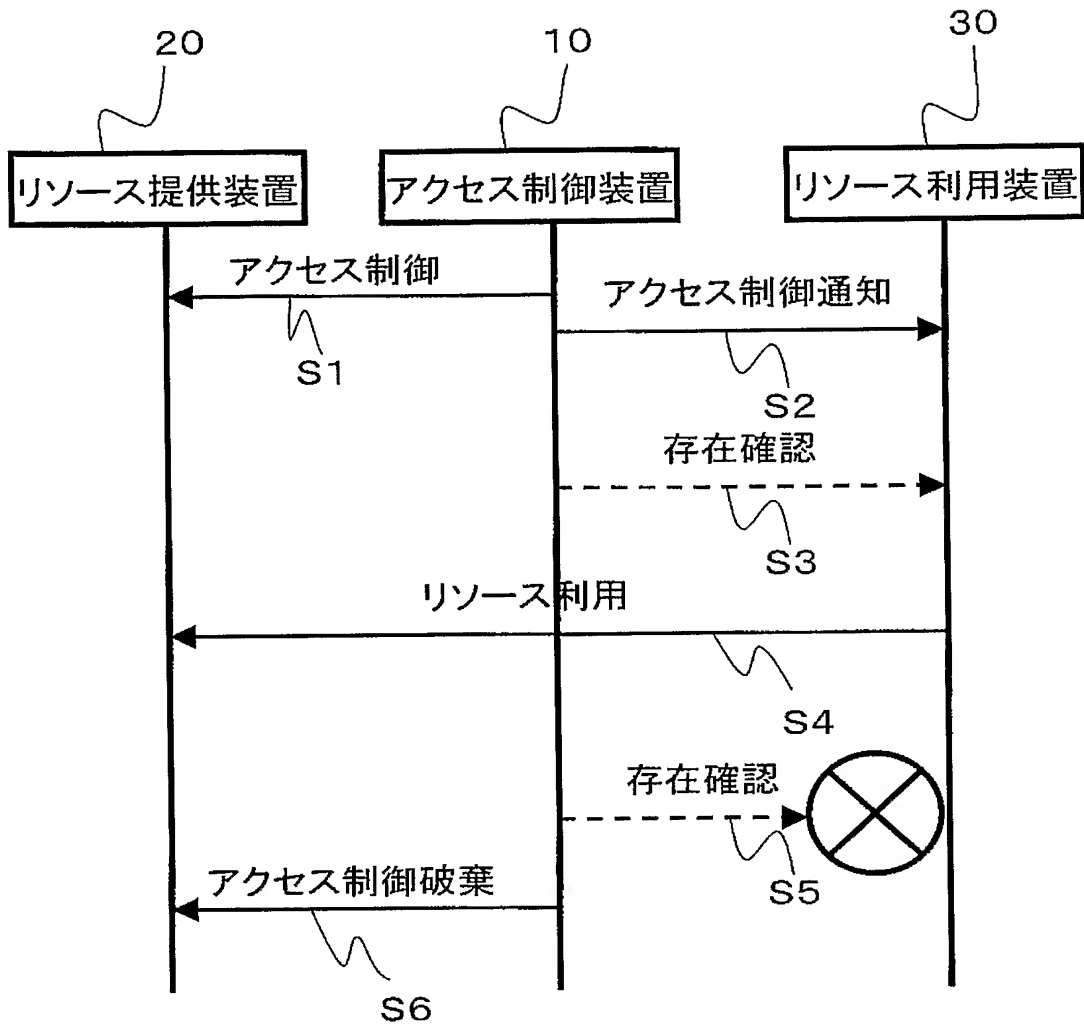
- 1 0 アクセス制御装置
- 2 0 リソース提供装置
- 3 0 リソース利用装置
- 4 0 アクセス制御装置 1 0 とリソース提供装置 2 0 との接続
- 5 0 リソース利用装置 3 0 とリソース提供装置 2 0 との接続
- 6 0 アクセス制御装置 1 0 とリソース利用装置 3 0 との接続
- 1 0 0 提供側の列
- 1 0 1 利用側の列
- 1 0 2 通信インターフェースの列
- 1 0 3 アクセスの列
- 2 0 0 制御側の列
- 2 0 1 アクセスの列

【書類名】図面

【図 1】



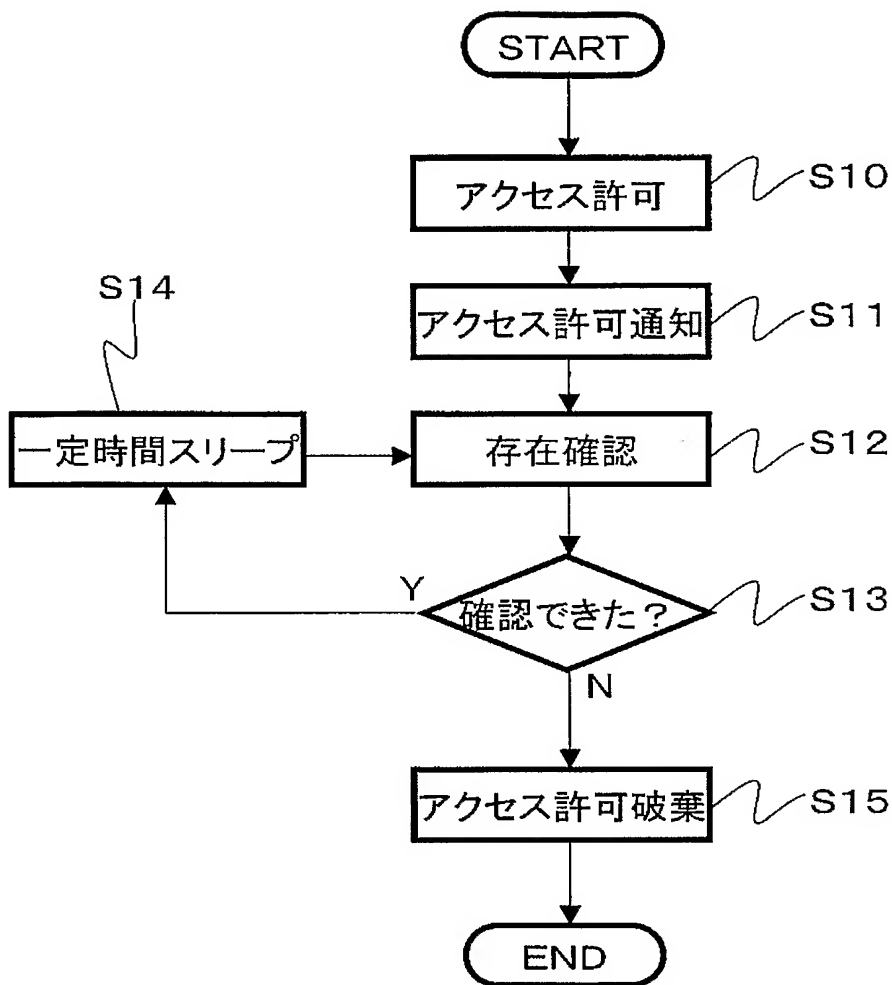
【図 2】



【図 3】

タイプ	
装置ID	
制御情報	コマンド名
	パラメータ制限

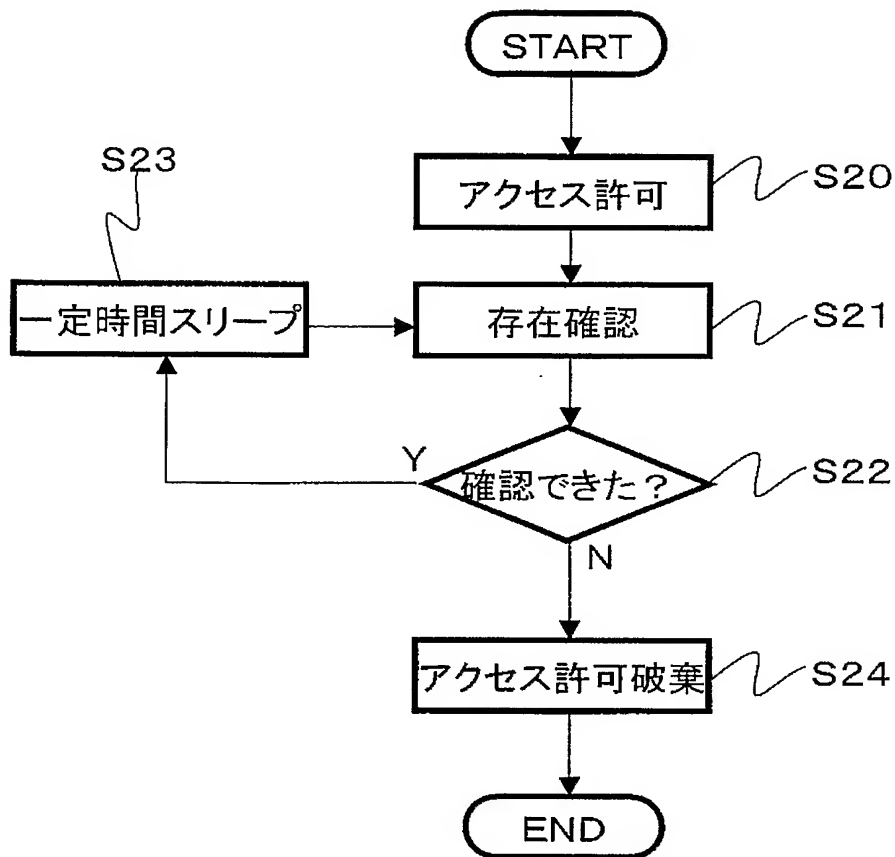
【図 4】



【図 5】

提供側	利用側	通信I/F	アクセス
携帯電話B	携帯電話E	eth0	秘密資料参照
据置機器C	携帯電話B	ANY	ビデオ視聴
パソコンD	携帯電話E	eth1	印刷
据置機器C	据置機器F	ttyS0	リモコン制御
パソコンD	パソコンG	eth0	ファイル書込み

【図 6】



【図 7】

制御側	アクセス
携帯電話H	秘密資料参照
携帯電話H	ビデオ視聴
据置機器I	印刷
据置機器I	リモコン制御
パソコンJ	ファイル書込み

【書類名】要約書

【要約】

【課題】 リソース提供装置 20 の不正利用を防止する。

【解決手段】 アクセス制御装置 10 は、リソース利用装置 30 からリソース提供装置 20 へのアクセスを許可するアクセス制御を行い、アクセス許可装置とリソース利用装置 30 との通信状態を監視し、リソース利用装置 30 とのリンク切断が確認された場合、前期アクセス制御を破棄する破棄制御をリソース提供装置 20 に対して行うことによって、リソース提供装置 20 の不正な使用を防止することができる。

【選択図】 図 1

特願 2 0 0 4 - 0 6 7 0 0 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社